IN THE CLAIMS

Please cancel claims 1-25 without prejudice or disclaimer, and substitute new claims 26-50 therefor as follows:

Claims 1-25 (Cancelled).

26. (New) An intrusion detection system for detecting unauthorised use of a network, comprising:

a sniffer for capturing data being transmitted on said network and a pattern matching engine receiving data captured by said sniffer and comparing said data with attack signatures for generating an event when a match between captured data and at least one attack signature is found; and

a response analysis engine, triggered by said event for comparing with response signatures the data being transmitted on said network as a response to said data matched with said attack signature and for correlating the results of said comparisons with attack and response signatures for generating an alarm.

27. (New) The system of claim 26, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by said sniffer by performing an analysis of source IP address in data packets transmitted on said network.

28. (New) The system of claim 26, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by said sniffer by performing an analysis of both source and destination IP addresses in data packets transmitted on said network.

29. (New) The system of claim 26, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by said sniffer by analysing transport level information in data packets transmitted on said network.

30. (New) The system of claim 26, wherein said response analysis engine generates an alarm when said data being transmitted on said network as a response to said data matched with said attack signature indicates that a new network connection has been established.

31. (New) The system of claim 26, wherein said response signatures are arranged in two categories, response signatures identifying an illicit traffic, and response signatures identifying legitimate traffic.

32. (New) The system of claim 31, wherein said response analysis engine generates an alarm when a match between captured data and a response signature identifying illicit traffic is found.

33. (New) The system of claim 31, wherein said response analysis engine comprises a counter which is incremented when a match between captured data and a response signature identifying legitimate traffic is found.

34. (New) The system of claim 33, wherein, when said counter reaches a predetermined value, said response analysis engine terminates without generating any alarm.

35. (New) The system of claim 26, wherein said response analysis engine comprises a time-out system triggered by said event for starting a probing task.

36. (New) The system of claim 35, wherein said probing task verifies if any data has been detected on said network as a response to said data matched with said attack signature and, if such condition is verified:

generates an alarm in case only response signatures indicating legitimate traffic have been used by said response analysis engine; or

ends the probing task in case only response signatures indicating illicit traffic or both response signatures indicating legitimate traffic and illicit traffic have been used by said response analysis engine.

37. (New) The system of claim 36, wherein, if such condition is not verified, said probing task attempts to perform a connection to a suspected attacked computer, for generating an alarm if such attempt is successful, or for ending the probing task if such attempt is unsuccessful.

38. (New) A method for detecting unauthorised use of a network, comprising the steps:

capturing data being transmitted on said network;

comparing said data with attack signatures for generating an event when a match between captured data and at least one attack signature is found; and when triggered by said event;

comparing with response signatures the data being transmitted on said network as a response to said data matched with said attack signature; and

correlating the results of said comparisons with attack and response signatures for generating an alarm.

39. (New) The method of claim 38, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by performing an analysis of source IP address in data packets transmitted on said network.

40. (New) The method of claim 38, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by performing an analysis of both source and destination IP addresses in data packets transmitted on said network.

41. (New) The method of claim 38, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by analysing transport level information in data packets transmitted on said network.

42. (New) The method of claim 38, comprising the step of generating an alarm when said data being transmitted on said network as a response to said data matched with said attack signature indicates that a new network connection has been established.

43. (New) The method of claim 38, wherein said response signatures are arranged in two categories, response signatures identifying illicit traffic, and response signatures identifying legitimate traffic.

44. (New) The method of claim 43, comprising the step of generating an alarm when a match between captured data and a response signature identifying illicit traffic is found.

45. (New) The method of claim 43, comprising the step of incrementing a counter when a match between captured data and a response signature identifying legitimate traffic is found.

46. (New) The method of claim 45, wherein said step of comparing data with response signatures is terminated when said counter reaches a predetermined value.

47. (New) The method of claim 38, comprising the step of providing a time-out system, triggered by said event, for starting a probing task.

48. (New) The method of claim 47, comprising the step of verifying if any data has been detected on said network as a response to said data matched with said attack signature, and, if such condition is verified:

generating an alarm in case only response signatures indicating legitimate traffic have been used; or

ending said probing task in case only response signatures indicating illicit traffic or both response signatures indicating legitimate traffic and illicit traffic have been used.

49. (New) The method of claim 48, wherein, if such condition is not verified, said probing task attempts to perform a connection to a suspected attacked computer, for generating an alarm if such attempt is successful, or for ending the probing task if such attempt is unsuccessful.

50. (New) A computer program product capable of being loaded in the memory of at least one computer and including software code portions for performing the method of any one of claims 38 to 49 when the product is capable of being run on a computer.